

(19) 日本国特許庁 (JP)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開2002-229447

(P2002-229447A)

(43) 公開日 平成14年8月14日 (2002.8.14)

| (51) Int.Cl. ⁷ | 識別記号 | F I | テマコード [*] (参考) |
|---------------------------|-------|--------------|-------------------------|
| G 09 C 1/00 | 6 4 0 | G 09 C 1/00 | 6 4 0 B 5 B 0 1 7 |
| G 06 F 12/14 | 3 1 0 | G 06 F 12/14 | 3 1 0 Z 5 B 0 3 5 |
| | 3 2 0 | | 3 2 0 B 5 B 0 5 8 |
| | | | 3 2 0 E 5 J 1 0 4 |
| G 06 K 17/00 | | G 06 K 17/00 | T |

審査請求 有 請求項の数14 O L (全14頁) 最終頁に続く

| | | | |
|-----------|---------------------------|----------|--|
| (21) 出願番号 | 特願2001-22179(P2001-22179) | (71) 出願人 | 000004226 日本電信電話株式会社 東京都千代田区大手町二丁目3番1号 |
| (22) 出願日 | 平成13年1月30日(2001.1.30) | (72) 発明者 | 松岡 寿延 東京都千代田区大手町二丁目3番1号 日本電信電話株式会社内 |
| | | (72) 発明者 | 堀 正弘 東京都千代田区大手町二丁目3番1号 日本電信電話株式会社内 |
| | | (74) 代理人 | 100083806 弁理士 三好 秀和 (外1名) |
| | | | |

最終頁に続く

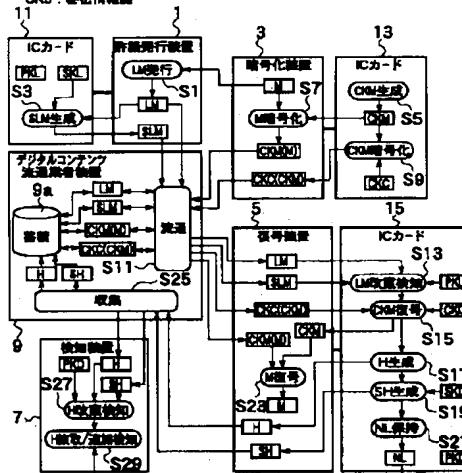
(54) 【発明の名称】 デジタルコンテンツ流通における著作権保護システム

(57) 【要約】

【課題】 デジタルコンテンツに対して発行された利用許諾情報の定める許諾範囲を逸脱してデジタルコンテンツが不正に利用されることを検知して防止するデジタルコンテンツ流通における著作権保護システムを提供する。

【解決手段】 許諾発行装置1はデジタルコンテンツMに対して許諾範囲を定義した利用許諾情報L Mを発行し、許諾発行装置秘密鍵S K Lで利用許諾情報L Mに対する許諾電子署名S L Mを許諾発行装置用ICカード1 1内で生成し、復号装置5は暗号化装置3においてコンテンツ鍵C K Mで暗号化されたデジタルコンテンツMを利用許諾情報L Mの定義する許諾範囲に従って復号装置用ICカード1 5内で復号するとともに、許諾発行装置1と共に共有する許諾発行装置公開鍵P K Lおよび許諾電子署名S L Mにより利用許諾情報L Mの不正改竄を復号装置用ICカード1 5内で検知する。

M : デジタルコンテンツ
LM : Mに対して発行された
利用許諾情報
SLM : LMに対する許諾電子署名
CKM : CKMで暗号化したMに対する
CKM : CKMに対するコンテンツ鍵
H : 錠錠用鍵
NL : 鍵を生成する最後の鍵を返し番号
SH : Hに対する鍵電子署名
SKL : 許諾発行装置秘密鍵
PKL : 許諾発行装置公開鍵
CRC : 暗号化装置
SKD : 復号装置秘密鍵
PKD : 復号装置公開鍵
CRK : 復号装置鍵



【特許請求の範囲】

【請求項1】 流通するデジタルコンテンツの不正利用を防止するデジタルコンテンツ流通における著作権保護システムであって、

デジタルコンテンツに対して許諾範囲を定義した利用許諾情報を発行する許諾発行装置であって、当該許諾発行装置に固有の許諾発行装置秘密鍵を保持している許諾発行装置秘密鍵保持手段、およびこの保持している許諾発行装置秘密鍵で前記利用許諾情報に対する許諾電子署名を生成して該利用許諾情報に付加する許諾電子署名生成付与手段を有する許諾発行装置と、

前記デジタルコンテンツに固有のコンテンツ鍵でデジタルコンテンツを暗号化する暗号化装置と、

前記許諾発行装置と共有する許諾発行装置公開鍵を保持する鍵保持手段、この保持している許諾発行装置公開鍵および前記利用許諾情報に付加された許諾電子署名により該利用許諾情報の不正改竄を検知する不正改竄検知手段、および前記コンテンツ鍵で暗号化されたデジタルコンテンツを前記利用許諾情報の定義する許諾範囲に従つて復号するコンテンツ復号手段を有する復号装置とを有することを特徴とするデジタルコンテンツ流通における著作権保護システム。

【請求項2】 前記暗号化装置は、

前記デジタルコンテンツに固有のコンテンツ鍵を生成するコンテンツ鍵生成手段、暗号化装置鍵を保持している暗号化装置鍵保持手段、およびこの保持している暗号化装置鍵で前記コンテンツ鍵を暗号化するコンテンツ鍵暗号化手段を更に有し、

前記復号装置の前記鍵保持手段が当該復号装置に固有の復号装置秘密鍵、前記暗号化装置と共有する暗号化装置鍵を更に保持しており、

前記復号装置は、

前記暗号化装置鍵で暗号化されたコンテンツ鍵を前記暗号化装置と共有する暗号化装置鍵で復号するコンテンツ鍵復号手段、この復号時に連続した自然数を履歴通し番号として含む鍵復号履歴を生成する鍵復号履歴生成手段、前記履歴通し番号を保持する履歴通し番号保持手段、および前記鍵保持手段に保持している復号装置秘密鍵で前記鍵復号履歴に履歴電子署名を付加する履歴電子署名付加手段を更に有することを特徴とする請求項1記載のデジタルコンテンツ流通における著作権保護システム。

【請求項3】 前記復号装置と共有する復号装置公開鍵および前記鍵復号履歴に付加された履歴電子署名により前記鍵復号履歴の不正改竄を検知する鍵復号履歴不正改竄検知手段、および前記鍵復号履歴に含まれる履歴通し番号の連続性および前記復号装置に保持している履歴通し番号の参照により鍵復号履歴の不正な抜き取りおよび不正な追加を検知する不正抜取／追加検知手段を有することを特徴とする請求項2記載の検知装置を更に有することを特徴とする請求項2記載の

デジタルコンテンツ流通における著作権保護システム。

【請求項4】 流通するデジタルコンテンツの不正利用を防止するデジタルコンテンツ流通における著作権保護システムであって、

デジタルコンテンツに対して許諾範囲を定義した利用許諾情報を発行する許諾発行装置であって、当該許諾発行装置に固有の許諾発行装置秘密鍵を保持している許諾発行装置秘密鍵保持手段、およびこの保持している許諾発行装置秘密鍵で前記利用許諾情報に対する許諾電子署名を生成して該利用許諾情報に付加する許諾電子署名生成手段を有する許諾発行装置と、

前記デジタルコンテンツに固有のコンテンツ鍵を生成するコンテンツ鍵生成手段、該コンテンツ鍵で前記デジタルコンテンツを暗号化するコンテンツ暗号化手段、暗号化装置鍵を保持している暗号化装置鍵保持手段、およびこの保持している暗号化装置鍵で前記コンテンツ鍵を暗号化するコンテンツ鍵暗号化手段を有する暗号化装置と、

前記許諾発行装置と共有する許諾発行装置公開鍵、復号装置に固有の復号装置秘密鍵、前記暗号化装置と共有する暗号化装置鍵を保持する鍵保持手段、この保持している許諾発行装置公開鍵および前記利用許諾情報に付加された許諾電子署名により該利用許諾情報の不正改竄を検知する利用許諾情報不正改竄検知手段、前記暗号化装置鍵で暗号化されたコンテンツ鍵を前記鍵保持手段に保持している暗号化装置鍵で復号するコンテンツ鍵復号手段、この復号時に連続した自然数を履歴通し番号として含む鍵復号履歴を生成する鍵復号履歴生成手段、前記履歴通し番号を保持する履歴通し番号保持手段、前記保持している復号装置秘密鍵で前記鍵復号履歴に履歴電子署名を付加する履歴電子署名付加手段、および前記復号されたコンテンツ鍵を用いて、前記コンテンツ鍵で暗号化されたデジタルコンテンツを前記利用許諾情報の定義する許諾範囲に従つて復号するコンテンツ復号手段を有する復号装置と、

前記復号装置と共有する復号装置公開鍵および前記鍵復号履歴に付加された履歴電子署名により前記鍵復号履歴の不正改竄を検知する鍵復号履歴不正改竄検知手段、および前記鍵復号履歴に含まれる履歴通し番号の連続性および前記復号装置に保持している履歴通し番号の参照により鍵復号履歴の不正な抜き取りおよび不正な追加を検知する不正抜取／追加検知手段を有する検知装置とを有することを特徴とするデジタルコンテンツ流通における著作権保護システム。

【請求項5】 前記暗号化装置の前記コンテンツ鍵生成手段、前記コンテンツ鍵暗号化手段、および前記暗号化装置鍵保持手段をタンパフリーアル性ハードウェアで構成し、コンテンツ鍵生成、コンテンツ鍵暗号化、および暗号化装置鍵保持を前記タンパフリーアル性ハードウェア内に閉じて実行することを特徴とする請求項4記載のデジタル

ルコンテンツ流通における著作権保護システム。

【請求項6】 前記許諾発行装置の前記許諾発行装置秘密鍵保持手段、および前記許諾電子署名生成付与手段をタンパフリー性ハードウェアで構成し、許諾発行装置秘密鍵保持および許諾電子署名生成付与を前記タンパフリー性ハードウェア内に閉じて実行することを特徴とする請求項4記載のデジタルコンテンツ流通における著作権保護システム。

【請求項7】 前記復号装置の前記鍵保持手段、前記利用許諾情報不正改竄検知手段、前記コンテンツ鍵復号手段、前記鍵復号履歴生成手段、前記履歴通し番号保持手段、前記履歴電子署名付加手段をタンパフリー性ハードウェアで構成し、鍵保持、利用許諾情報不正改竄検知、コンテンツ鍵復号、鍵復号履歴生成、履歴通し番号保持、履歴電子署名付加をタンパフリー性ハードウェア内に閉じて実行することを特徴とする請求項4記載のデジタルコンテンツ流通における著作権保護システム。

【請求項8】 前記暗号化装置、許諾発行装置、および復号装置は、秘密情報鍵を共有し、前記暗号化装置は、前記暗号化装置鍵を前記秘密情報鍵で暗号化して保持する手段を有し、前記許諾発行装置は、前記許諾発行装置秘密鍵を前記秘密情報鍵で暗号化して保持する手段を有し、前記復号装置は、前記暗号化装置鍵、復号装置秘密鍵、履歴通し番号を前記秘密情報鍵で暗号化して保持する手段を有することを特徴とする請求項4記載のデジタルコンテンツ流通における著作権保護システム。

【請求項9】 前記暗号化装置の前記コンテンツ鍵生成手段、前記コンテンツ鍵暗号化手段、および前記暗号化装置鍵保持手段をタンパフリー性ハードウェアで構成し、コンテンツ鍵生成、コンテンツ鍵暗号化、および暗号化装置鍵保持を前記タンパフリー性ハードウェア内に閉じて実行し、

前記許諾発行装置および復号装置は、秘密情報鍵を共有し、

前記許諾発行装置は、前記許諾発行装置秘密鍵を前記秘密情報鍵で暗号化して保持する手段を有し、

前記復号装置は、前記暗号化装置鍵、復号装置秘密鍵、履歴通し番号を前記秘密情報鍵で暗号化して保持する手段を有することを特徴とする請求項4記載のデジタルコンテンツ流通における著作権保護システム。

【請求項10】 前記許諾発行装置の前記許諾発行装置秘密鍵保持手段、および前記許諾電子署名生成付与手段をタンパフリー性ハードウェアで構成し、許諾発行装置秘密鍵保持手段および許諾電子署名生成付与を前記タンパフリー性ハードウェア内に閉じて実行し、

前記暗号化装置および復号装置は、秘密情報鍵を共有し、

前記暗号化装置は、前記暗号化装置鍵を前記秘密情報鍵で暗号化して保持する手段を有し、

前記復号装置は、前記暗号化装置鍵、復号装置秘密鍵、履歴通し番号を前記秘密情報鍵で暗号化して保持する手段を有することを特徴とする請求項4記載のデジタルコンテンツ流通における著作権保護システム。

【請求項11】 前記復号装置の前記鍵保持手段、前記利用許諾情報不正改竄検知手段、前記コンテンツ鍵復号手段、前記鍵復号履歴生成手段、前記履歴通し番号保持手段、前記履歴電子署名付加手段をタンパフリー性ハードウェアで構成し、鍵保持、利用許諾情報不正改竄検知、コンテンツ鍵復号、鍵復号履歴生成、履歴通し番号保持、履歴電子署名付加をタンパフリー性ハードウェア内に閉じて実行し、

前記暗号化装置および許諾発行装置は、秘密情報鍵を共有し、

前記暗号化装置は、前記暗号化装置鍵を前記秘密情報鍵で暗号化して保持する手段を有し、

前記許諾発行装置は、前記許諾発行装置秘密鍵を前記秘密情報鍵で暗号化して保持する手段を有することを特徴とする請求項4記載のデジタルコンテンツ流通における著作権保護システム。

【請求項12】 前記暗号化装置は、暗号化装置鍵を前記秘密情報鍵で暗号化して保持する手段を有し、前記許諾発行装置の前記許諾発行装置秘密鍵保持手段および前記許諾電子署名生成付与手段をタンパフリー性ハードウェアで構成し、許諾発行装置秘密鍵保持および許諾電子署名生成付与を前記タンパフリー性ハードウェア内に閉じて実行し、

前記復号装置の前記鍵保持手段、前記利用許諾情報不正改竄検知手段、前記コンテンツ鍵復号手段、前記鍵復号履歴生成手段、前記履歴通し番号保持手段、前記履歴電子署名付加手段をタンパフリー性ハードウェアで構成し、鍵保持、利用許諾情報不正改竄検知、コンテンツ鍵復号、鍵復号履歴生成、履歴通し番号保持、履歴電子署名付加をタンパフリー性ハードウェア内に閉じて実行することを特徴とする請求項4記載のデジタルコンテンツ流通における著作権保護システム。

【請求項13】 前記許諾発行装置は、前記許諾発行装置秘密鍵を秘密情報鍵で暗号化して保持する手段を有し、

前記暗号化装置の前記コンテンツ鍵生成手段、前記コンテンツ鍵暗号化手段、および前記暗号化装置鍵保持手段をタンパフリー性ハードウェアで構成し、コンテンツ鍵生成、コンテンツ鍵暗号化、および暗号化装置鍵保持を前記タンパフリー性ハードウェア内に閉じて実行し、

前記復号装置の前記鍵保持手段、前記利用許諾情報不正改竄検知手段、前記コンテンツ鍵復号手段、前記鍵復号履歴生成手段、前記履歴通し番号保持手段、前記履歴電子署名付加手段をタンパフリー性ハードウェアで構成し、鍵保持、利用許諾情報不正改竄検知、コンテンツ鍵復号、鍵復号履歴生成、履歴通し番号保持、履歴電子署

名付加をタンパフリー性ハードウェア内に閉じて実行することを特徴とする請求項4記載のデジタルコンテンツ流通における著作権保護システム。

【請求項14】前記復号装置は、前記暗号化装置鍵、復号装置秘密鍵、履歴通し番号を前記秘密情報鍵で暗号化して保持する手段を有し、前記暗号化装置の前記コンテンツ鍵生成手段、前記コンテンツ鍵暗号化手段、および前記暗号化装置鍵保持手段をタンパフリー性ハードウェアで構成し、コンテンツ鍵生成、コンテンツ鍵暗号化、および暗号化装置鍵保持を前記タンパフリー性ハードウェア内に閉じて実行し、前記許諾発行装置の前記許諾発行装置秘密鍵保持手段、および前記許諾電子署名生成付与手段をタンパフリー性ハードウェアで構成し、許諾発行装置秘密鍵保持および許諾電子署名生成付与を前記タンパフリー性ハードウェア内に閉じて実行することを特徴とする請求項4記載のデジタルコンテンツ流通における著作権保護システム。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、流通するデジタルコンテンツの不正利用を防止するデジタルコンテンツ流通における著作権保護システムに関し、詳しくは、ネットワークまたはデジタル記録媒体を介して流通するデジタルコンテンツが当該コンテンツに対して発行された利用許諾情報の定める許諾範囲を逸脱して不正に利用されることを検知して防止するデジタルコンテンツ流通における著作権保護システムに関する。

【0002】

【従来の技術】デジタルコンテンツ流通サービスにおいては、デジタルコンテンツの複製の容易性のため、デジタルコンテンツに対して定められた許諾範囲を逸脱した不正利用を検知して防止する技術が必須である。この技術は、具体的には以下に記載する2つの技術から構成される。

【0003】すなわち、第1の技術は、デジタルコンテンツの許諾範囲を定める利用許諾情報を改竄を検知する技術およびこの許諾範囲を逸脱する不正利用を防止する技術であり、第2の技術は、デジタルコンテンツの利用時の利用履歴生成および利用履歴検証による不正利用の検知技術である。

【0004】

【発明が解決しようとする課題】上述した技術のうち、第1の技術においては、デジタルコンテンツに利用許諾情報を付随する場合には、この利用許諾情報の不正改竄による不正利用という問題があり、また利用許諾情報をセンタで管理する場合には、ネットワーク上の相互認証通信によるトラヒックの増加およびサービスコストの増加、ネットワーク非接続時のコンテンツ利用不可という問題がある。

【0005】また、第2の技術においては、利用履歴の

改竄や抜き取りによる不正利用という問題があることに加えて、この利用履歴をセンタで管理する場合には、ネットワーク上の相互認証通信によるトラヒックの増加およびサービスコストの増加、ネットワーク非接続時のコンテンツ利用不可という問題がある。

【0006】本発明は、上記に鑑みてなされたもので、その目的とするところは、デジタルコンテンツに対して発行された利用許諾情報の定める許諾範囲を逸脱してデジタルコンテンツが不正に利用されることを検知して防止するデジタルコンテンツ流通における著作権保護システムを提供することにある。

【0007】

【課題を解決するための手段】上記目的を達成するため、請求項1記載の本発明は、流通するデジタルコンテンツの不正利用を防止するデジタルコンテンツ流通における著作権保護システムであって、デジタルコンテンツに対して許諾範囲を定義した利用許諾情報を発行する許諾発行装置であって、当該許諾発行装置に固有の許諾発行装置秘密鍵を保持している許諾発行装置秘密鍵保持手段、およびこの保持している許諾発行装置秘密鍵で前記利用許諾情報に対する許諾電子署名を生成して該利用許諾情報に付加する許諾電子署名生成付与手段を有する許諾発行装置と、前記デジタルコンテンツに固有のコンテンツ鍵でデジタルコンテンツを暗号化する暗号化装置と、前記許諾発行装置と共有する許諾発行装置公開鍵を保持する鍵保持手段、この保持している許諾発行装置公開鍵および前記利用許諾情報に付加された許諾電子署名により該利用許諾情報の不正改竄を検知する不正改竄検知手段、および前記コンテンツ鍵で暗号化されたデジタルコンテンツを前記利用許諾情報の定義する許諾範囲に従って復号するコンテンツ復号手段を有する復号装置とを有することを要旨とする。

【0008】請求項1記載の本発明にあっては、許諾発行装置はデジタルコンテンツに対して許諾範囲を定義した利用許諾情報を発行し、許諾発行装置に固有の許諾発行装置秘密鍵で利用許諾情報に対する許諾電子署名を生成し、復号装置は暗号化装置においてコンテンツ鍵で暗号化されたデジタルコンテンツを利用許諾情報の定義する許諾範囲に従って復号するとともに、許諾発行装置と共有する許諾発行装置公開鍵および許諾電子署名により利用許諾情報の不正改竄を検知するため、デジタルコンテンツを許諾範囲内のみで利用可能とし、許諾範囲を逸脱した不正利用を検知して防止することができ、またネットワーク上の相互認証通信によるトラヒックの増加およびサービスコストの増加、ネットワーク非接続時のコンテンツ利用不可という従来の問題を解決できる。また、復号装置は復号時に許諾発行装置などの外部と接続されている必要がない。

【0009】また、請求項2記載の本発明は、請求項1記載の発明において、前記暗号化装置が、前記デジタル

コンテンツに固有のコンテンツ鍵を生成するコンテンツ鍵生成手段、暗号化装置鍵を保持している暗号化装置鍵保持手段、およびこの保持している暗号化装置鍵で前記コンテンツ鍵を暗号化するコンテンツ鍵暗号化手段を更に有し、前記復号装置の前記鍵保持手段が当該復号装置に固有の復号装置秘密鍵、前記暗号化装置と共有する暗号化装置鍵を更に保持しており、前記復号装置は、前記保持されている暗号化装置鍵で暗号化されたコンテンツ鍵を前記暗号化装置と共有する暗号化装置鍵で復号するコンテンツ鍵復号手段、この復号時に連続した自然数を履歴通し番号として含む鍵復号履歴を生成する鍵復号履歴生成手段、前記履歴通し番号を保持する履歴通し番号保持手段、および前記鍵保持手段に保持している復号装置秘密鍵で前記鍵復号履歴に履歴電子署名を付加する履歴電子署名付加手段を更に有することを要旨とする。

【0010】請求項2記載の本発明にあっては、暗号化装置はデジタルコンテンツに固有のコンテンツ鍵を生成し、暗号化装置鍵でコンテンツ鍵を暗号化し、復号装置は暗号化されたコンテンツ鍵を暗号化装置鍵で復号し、この復号時に連続した自然数を履歴通し番号として含む鍵復号履歴を生成し、履歴通し番号を保持し、復号装置秘密鍵で鍵復号履歴に履歴電子署名を付加する。

【0011】更に、請求項3記載の本発明は、請求項2記載の発明において、前記復号装置と共有する復号装置公開鍵および前記鍵復号履歴に付加された履歴電子署名により前記鍵復号履歴の不正改竄を検知する鍵復号履歴不正改竄検知手段、および前記鍵復号履歴に含まれる履歴通し番号の連続性および前記復号装置に保持している履歴通し番号の参照により鍵復号履歴の不正な抜き取りおよび不正な追加を検知する不正抜取／追加検知手段を有する検知装置を更に有することを要旨とする。

【0012】請求項3記載の本発明にあっては、検知装置は復号装置公開鍵および鍵復号履歴に付加された履歴電子署名により鍵復号履歴の不正改竄を検知し、鍵復号履歴に含まれる履歴通し番号の連続性および復号装置に保持している履歴通し番号の参照により鍵復号履歴の不正な抜き取りおよび不正な追加を検知するため、デジタルコンテンツ流通業者の水増し請求やデジタルコンテンツ利用者の利用否認による支払い拒否などを防止することができる。また、検知装置による鍵復号履歴の収集は復号時である必要はなく、復号装置は復号時に検知装置に接続されている必要がない。

【0013】請求項4記載の本発明は、流通するデジタルコンテンツの不正利用を防止するデジタルコンテンツ流通における著作権保護システムであって、デジタルコンテンツに対して許諾範囲を定義した利用許諾情報を発行する許諾発行装置であって、当該許諾発行装置に固有の許諾発行装置秘密鍵を保持している許諾発行装置秘密鍵保持手段、およびこの保持している許諾発行装置秘密鍵で前記利用許諾情報に対する許諾電子署名を生成して

該利用許諾情報に付加する許諾電子署名生成手段を有する許諾発行装置と、前記デジタルコンテンツに固有のコンテンツ鍵を生成するコンテンツ鍵生成手段、該コンテンツ鍵で前記デジタルコンテンツを暗号化するコンテンツ暗号化手段、暗号化装置鍵を保持している暗号化装置鍵保持手段、およびこの保持している暗号化装置鍵で前記コンテンツ鍵を暗号化するコンテンツ鍵暗号化手段を有する暗号化装置と、前記許諾発行装置と共有する許諾発行装置公開鍵、復号装置に固有の復号装置秘密鍵、前記暗号化装置と共有する暗号化装置鍵を保持する鍵保持手段、この保持している許諾発行装置公開鍵および前記利用許諾情報に付加された許諾電子署名により該利用許諾情報の不正改竄を検知する利用許諾情報不正改竄検知手段、前記暗号化装置鍵で暗号化されたコンテンツ鍵を前記鍵保持手段に保持している暗号化装置鍵で復号するコンテンツ鍵復号手段、この復号時に連続した自然数を履歴通し番号として含む鍵復号履歴を生成する鍵復号履歴生成手段、前記履歴通し番号を保持する履歴通し番号保持手段、前記保持している復号装置秘密鍵で前記鍵復号履歴に履歴電子署名を付加する履歴電子署名付加手段、および前記復号されたコンテンツ鍵を用いて、前記コンテンツ鍵で暗号化されたデジタルコンテンツを前記利用許諾情報の定義する許諾範囲に従って復号するコンテンツ復号手段を有する復号装置と、前記復号装置と共有する復号装置公開鍵および前記鍵復号履歴に付加された履歴電子署名により前記鍵復号履歴の不正改竄を検知する鍵復号履歴不正改竄検知手段、および前記鍵復号履歴に含まれる履歴通し番号の連続性および前記復号装置に保持している履歴通し番号の参照により鍵復号履歴の不正な抜き取りおよび不正な追加を検知する不正抜取／追加検知手段を有する検知装置とを有することを要旨とする。

【0014】請求項4記載の本発明にあっては、許諾発行装置はデジタルコンテンツに対して許諾範囲を定義した利用許諾情報を発行し、許諾発行装置秘密鍵で利用許諾情報に対する許諾電子署名を生成し、暗号化装置はデジタルコンテンツに固有のコンテンツ鍵を生成し、該コンテンツ鍵でデジタルコンテンツを暗号化し、暗号化装置鍵でコンテンツ鍵を暗号化し、復号装置は許諾発行装置公開鍵および利用許諾情報に付加された許諾電子署名により利用許諾情報の不正改竄を検知し、暗号化されたコンテンツ鍵を暗号化装置鍵で復号し、この復号時に連続した自然数を履歴通し番号として含む鍵復号履歴を生成し、履歴通し番号を保持し、復号装置秘密鍵で鍵復号履歴に履歴電子署名を付加し、暗号化されたデジタルコンテンツをコンテンツ鍵で利用許諾情報の定義する許諾範囲に従って復号し、検知装置は復号装置公開鍵および鍵復号履歴に付加された履歴電子署名により鍵復号履歴の不正改竄を検知し、鍵復号履歴に含まれる履歴通し番号の連続性および復号装置に保持している履歴通し番号

の参照により鍵復号履歴の不正な抜き取りおよび不正な追加を検知するため、デジタルコンテンツを許諾範囲内のみで利用可能とし、許諾範囲を逸脱した不正利用を検知して防止することができ、デジタルコンテンツ流通業者の水増し請求やデジタルコンテンツ利用者の利用否認による支払い拒否などを防止することができるとともに、コンテンツ利用後の利用履歴抜き取りまたは改竄によるデジタルコンテンツの不正利用を検知して防止でき、またネットワーク上の相互認証通信によるトラヒックの増加およびサービスコストの増加、ネットワーク非接続時のコンテンツ利用不可という従来の問題を解決できる。

【0015】また、請求項5記載の本発明は、請求項4記載の発明において、前記暗号化装置の前記コンテンツ鍵生成手段、前記コンテンツ鍵暗号化手段、および前記暗号化装置鍵保持手段をタンパフリーアル性ハードウェアで構成し、コンテンツ鍵生成、コンテンツ鍵暗号化、および暗号化装置鍵保持を前記タンパフリーアル性ハードウェア内に閉じて実行することを要旨とする。

【0016】請求項5記載の本発明にあっては、暗号化装置はコンテンツ鍵生成、コンテンツ鍵暗号化、および暗号化装置鍵保持をタンパフリーアル性ハードウェア内に閉じて実行するため、暗号化装置のセキュリティを高め、その不正防止効果を向上することができる。

【0017】更に、請求項6記載の本発明は、請求項4記載の発明において、前記許諾発行装置の前記許諾発行装置秘密鍵保持手段、および前記許諾電子署名生成付与手段をタンパフリーアル性ハードウェアで構成し、許諾発行装置秘密鍵保持および許諾電子署名生成付与を前記タンパフリーアル性ハードウェア内に閉じて実行することを要旨とする。

【0018】請求項6記載の本発明にあっては、許諾発行装置は許諾発行装置秘密鍵保持および許諾電子署名生成付与をタンパフリーアル性ハードウェア内に閉じて実行するため、許諾発行装置のセキュリティを高め、その不正防止効果を向上することができる。

【0019】請求項7記載の本発明は、請求項4記載の発明において、前記復号装置の前記鍵保持手段、前記利用許諾情報不正改竄検知手段、前記コンテンツ鍵復号手段、前記鍵復号履歴生成手段、前記履歴通し番号保持手段、前記履歴電子署名付加手段をタンパフリーアル性ハードウェアで構成し、鍵保持、利用許諾情報不正改竄検知、コンテンツ鍵復号、鍵復号履歴生成、履歴通し番号保持、履歴電子署名付加をタンパフリーアル性ハードウェア内に閉じて実行することを要旨とする。

【0020】請求項7記載の本発明にあっては、復号装置は鍵保持、利用許諾情報不正改竄検知、コンテンツ鍵復号、鍵復号履歴生成、履歴通し番号保持、履歴電子署名付加をタンパフリーアル性ハードウェア内に閉じて実行するため、復号装置のセキュリティを高め、その不正防止

効果を向上することができる。

【0021】また、請求項8記載の本発明は、請求項4記載の発明において、前記暗号化装置、許諾発行装置、および復号装置は、秘密情報鍵を共有し、前記暗号化装置は、前記暗号化装置鍵を前記秘密情報鍵で暗号化して保持する手段を有し、前記許諾発行装置は、前記許諾発行装置秘密鍵を前記秘密情報鍵で暗号化して保持する手段を有し、前記復号装置は、前記暗号化装置鍵、復号装置秘密鍵、履歴通し番号を前記秘密情報鍵で暗号化して保持する手段を有することを要旨とする。

【0022】請求項8記載の本発明にあっては、暗号化装置、許諾発行装置、および復号装置は、秘密情報鍵を共有し、暗号化装置鍵を秘密情報鍵で暗号化して保持し、許諾発行装置は許諾発行装置秘密鍵を秘密情報鍵で暗号化して保持し、復号装置は暗号化装置鍵、復号装置秘密鍵、履歴通し番号を秘密情報鍵で暗号化して保持するため、暗号化装置、許諾発行装置、および復号装置のそれぞれのセキュリティを高め、その不正防止効果を向上することができる。

【0023】更に、請求項9記載の本発明は、請求項4記載の発明において、前記暗号化装置の前記コンテンツ鍵生成手段、前記コンテンツ鍵暗号化手段、および前記暗号化装置鍵保持手段をタンパフリーアル性ハードウェアで構成し、コンテンツ鍵生成、コンテンツ鍵暗号化、および暗号化装置鍵保持を前記タンパフリーアル性ハードウェア内に閉じて実行し、前記許諾発行装置および復号装置は、秘密情報鍵を共有し、前記許諾発行装置は、前記許諾発行装置秘密鍵を前記秘密情報鍵で暗号化して保持する手段を有し、前記復号装置は、前記暗号化装置鍵、復号装置秘密鍵、履歴通し番号を前記秘密情報鍵で暗号化して保持する手段を有することを要旨とする。

【0024】請求項9記載の本発明にあっては、暗号化装置はコンテンツ鍵生成、コンテンツ鍵暗号化、および暗号化装置鍵保持をタンパフリーアル性ハードウェア内に閉じて実行し、許諾発行装置および復号装置は秘密情報鍵を共有し、許諾発行装置は許諾発行装置秘密鍵を秘密情報鍵で暗号化して保持し、復号装置は暗号化装置鍵、復号装置秘密鍵、履歴通し番号を秘密情報鍵で暗号化して保持するため、暗号化装置、許諾発行装置、および復号装置のそれぞれのセキュリティを高め、その不正防止効果を向上することができる。

【0025】請求項10記載の本発明は、請求項4記載の発明において、前記許諾発行装置の前記許諾発行装置秘密鍵保持手段、および前記許諾電子署名生成付与手段をタンパフリーアル性ハードウェアで構成し、許諾発行装置秘密鍵保持手段および許諾電子署名生成付与を前記タンパフリーアル性ハードウェア内に閉じて実行し、前記暗号化装置および復号装置は、秘密情報鍵を共有し、前記暗号化装置は、前記暗号化装置鍵を前記秘密情報鍵で暗号化して保持する手段を有し、前記復号装置は、前記暗号化

装置鍵、復号装置秘密鍵、履歴通し番号を前記秘密情報鍵で暗号化して保持する手段を有することを要旨とする。

【0026】請求項10記載の本発明にあっては、許諾発行装置は許諾発行装置秘密鍵保持手段および許諾電子署名生成付与をタンパフリー性ハードウェア内に閉じて実行し、暗号化装置および復号装置は秘密情報鍵を共有し、暗号化装置は暗号化装置鍵を秘密情報鍵で暗号化して保持し、復号装置は暗号化装置鍵、復号装置秘密鍵、履歴通し番号を秘密情報鍵で暗号化して保持するため、暗号化装置、許諾発行装置、および復号装置のそれぞれのセキュリティを高め、その不正防止効果を向上することができる。

【0027】請求項11記載の本発明は、請求項4記載の発明において、前記復号装置の前記鍵保持手段、前記利用許諾情報不正改竄検知手段、前記コンテンツ鍵復号手段、前記鍵復号履歴生成手段、前記履歴通し番号保持手段、前記履歴電子署名付加手段をタンパフリー性ハードウェアで構成し、鍵保持、利用許諾情報不正改竄検知、コンテンツ鍵復号、鍵復号履歴生成、履歴通し番号保持、履歴電子署名付加をタンパフリー性ハードウェア内に閉じて実行し、前記暗号化装置および許諾発行装置は、秘密情報鍵を共有し、前記暗号化装置は、前記暗号化装置鍵を前記秘密情報鍵で暗号化して保持する手段を有し、前記許諾発行装置は、前記許諾発行装置秘密鍵を前記秘密情報鍵で暗号化して保持する手段を有することを要旨とする。

【0028】請求項11記載の本発明にあっては、復号装置は鍵保持、利用許諾情報不正改竄検知、コンテンツ鍵復号、鍵復号履歴生成、履歴通し番号保持、履歴電子署名付加をタンパフリー性ハードウェア内に閉じて実行し、暗号化装置および許諾発行装置は秘密情報鍵を共有し、暗号化装置は暗号化装置鍵を前記秘密情報鍵で暗号化して保持し、許諾発行装置は許諾発行装置秘密鍵を秘密情報鍵で暗号化して保持するため、暗号化装置、許諾発行装置、および復号装置のそれぞれのセキュリティを高め、その不正防止効果を向上することができる。

【0029】更に、請求項12記載の本発明は、請求項4記載の発明において、前記暗号化装置は、暗号化装置鍵を前記秘密情報鍵で暗号化して保持する手段を有し、前記許諾発行装置の前記許諾発行装置秘密鍵保持手段および前記許諾電子署名生成付与手段をタンパフリー性ハードウェアで構成し、許諾発行装置秘密鍵保持および許諾電子署名生成付与を前記タンパフリー性ハードウェア内に閉じて実行し、前記復号装置の前記鍵保持手段、前記利用許諾情報不正改竄検知手段、前記コンテンツ鍵復号手段、前記鍵復号履歴生成手段、前記履歴通し番号保持手段、前記履歴電子署名付加手段をタンパフリー性ハードウェアで構成し、鍵保持、利用許諾情報不正改竄検知、コンテンツ鍵復号、鍵復号履歴生成、履歴通し番号保持、履歴電子署名付加をタンパフリー性ハードウェア内に閉じて実行することができる。

保持、履歴電子署名付加をタンパフリー性ハードウェア内に閉じて実行することを要旨とする。

【0030】請求項12記載の本発明にあっては、暗号化装置は暗号化装置鍵を秘密情報鍵で暗号化して保持し、許諾発行装置は許諾発行装置秘密鍵保持および許諾電子署名生成付与を前記タンパフリー性ハードウェア内に閉じて実行し、復号装置は鍵保持、利用許諾情報不正改竄検知、コンテンツ鍵復号、鍵復号履歴生成、履歴通し番号保持、履歴電子署名付加をタンパフリー性ハードウェア内に閉じて実行するため、暗号化装置、許諾発行装置、および復号装置のそれぞれのセキュリティを高め、その不正防止効果を向上することができる。

【0031】請求項13記載の本発明は、請求項4記載の発明において、前記許諾発行装置は、前記許諾発行装置秘密鍵を秘密情報鍵で暗号化して保持する手段を有し、前記暗号化装置の前記コンテンツ鍵生成手段、前記コンテンツ鍵暗号化手段、および前記暗号化装置鍵保持手段をタンパフリー性ハードウェアで構成し、コンテンツ鍵生成、コンテンツ鍵暗号化、および暗号化装置鍵保持を前記タンパフリー性ハードウェア内に閉じて実行し、前記復号装置の前記鍵保持手段、前記利用許諾情報不正改竄検知手段、前記コンテンツ鍵復号手段、前記鍵復号履歴生成手段、前記履歴通し番号保持手段、前記履歴電子署名付加手段をタンパフリー性ハードウェアで構成し、鍵保持、利用許諾情報不正改竄検知、コンテンツ鍵復号、鍵復号履歴生成、履歴通し番号保持、履歴電子署名付加をタンパフリー性ハードウェア内に閉じて実行することを要旨とする。

【0032】請求項13記載の本発明にあっては、許諾発行装置は許諾発行装置秘密鍵を秘密情報鍵で暗号化して保持し、暗号化装置はコンテンツ鍵生成、コンテンツ鍵暗号化、および暗号化装置鍵保持を前記タンパフリー性ハードウェア内に閉じて実行し、復号装置は鍵保持、利用許諾情報不正改竄検知、コンテンツ鍵復号、鍵復号履歴生成、履歴通し番号保持、履歴電子署名付加をタンパフリー性ハードウェア内に閉じて実行するため、暗号化装置、許諾発行装置、および復号装置のセキュリティを高め、その不正防止効果を向上することができる。

【0033】また、請求項14記載の本発明は、請求項4記載の発明において、前記復号装置が、前記暗号化装置鍵、復号装置秘密鍵、履歴通し番号を前記秘密情報鍵で暗号化して保持する手段を有し、前記暗号化装置の前記コンテンツ鍵生成手段、前記コンテンツ鍵暗号化手段、および前記暗号化装置鍵保持手段をタンパフリー性ハードウェアで構成し、コンテンツ鍵生成、コンテンツ鍵暗号化、および暗号化装置鍵保持を前記タンパフリー性ハードウェア内に閉じて実行し、前記許諾発行装置の前記許諾発行装置秘密鍵保持手段、および前記許諾電子署名生成付与手段をタンパフリー性ハードウェアで構成

し、許諾発行装置秘密鍵保持および許諾電子署名生成付与を前記タンパフリー性ハードウェア内に閉じて実行することを要旨とする。

【0034】請求項14記載の本発明にあっては、復号装置は暗号化装置鍵、復号装置秘密鍵、履歴通し番号を前記秘密情報鍵で暗号化して保持し、暗号化装置はコンテンツ鍵生成、コンテンツ鍵暗号化、および暗号化装置鍵保持を前記タンパフリー性ハードウェア内に閉じて実行し、許諾発行装置は許諾発行装置秘密鍵保持および許諾電子署名生成付与を前記タンパフリー性ハードウェア内に閉じて実行するため、暗号化装置、許諾発行装置、および復号装置のそれぞれのセキュリティを高め、その不正防止効果を向上することができる。

【0035】

【発明の実施の形態】以下、図面を用いて本発明の実施の形態を説明する。図1は、本発明の一実施形態に係るデジタルコンテンツ流通における著作権保護システムの構成を示す図である。同図に示す著作権保護システムは、許諾発行装置用ICカード11が接続された許諾発行装置1、暗号化装置用ICカード13が接続された暗号化装置3、復号装置用ICカード15が接続された復号装置5、検知装置7、およびデジタルコンテンツ流通業者装置9から構成されている。

【0036】許諾発行装置1および許諾発行装置用ICカード11は、互いにシリアルケーブルまたはUSBケーブルなどの汎用的なインターフェースで接続され、例えば音楽デジタルコンテンツMに対して許諾範囲を定義した利用許諾情報LMを発行する利用許諾情報発行手段、当該許諾発行装置1に固有の許諾発行装置秘密鍵SKLおよび許諾発行装置公開鍵PKLを保持している許諾発行装置秘密鍵保持手段、およびこの保持している許諾発行装置秘密鍵SKLで利用許諾情報LMに対する許諾電子署名SLMを生成して利用許諾情報LMに付加する許諾電子署名生成手段を有し、これらの手段のうち、許諾発行装置秘密鍵保持手段および許諾電子署名生成付与手段をタンパフリー性ハードウェアである許諾発行装置用ICカード11で構成し、これにより許諾発行装置秘密鍵保持および許諾電子署名生成付与をタンパフリー性ハードウェアである許諾発行装置用ICカード11内に閉じて実行して、許諾発行装置のセキュリティを高め、その不正防止効果を向上している。

【0037】また、暗号化装置3および暗号化装置用ICカード13は、互いにシリアルケーブルまたはUSBケーブルなどの汎用的なインターフェースで接続され、デジタルコンテンツMに固有のコンテンツ鍵CKMを生成するコンテンツ鍵生成手段、該コンテンツ鍵CKMでデジタルコンテンツMを暗号化するコンテンツ暗号化手段、暗号化装置鍵CKCを保持している暗号化装置鍵保持手段、およびこの保持している暗号化装置鍵CKCでコンテンツ鍵CKMを暗号化するコンテンツ鍵暗号化手

段を有し、この手段のうち、コンテンツ鍵生成手段、コンテンツ鍵暗号化手段、および暗号化装置鍵保持手段をタンパフリー性ハードウェアである暗号化装置用ICカード13で構成し、これによりコンテンツ鍵生成、コンテンツ鍵暗号化、および暗号化装置鍵保持をタンパフリー性ハードウェアである暗号化装置用ICカード13内に閉じて実行して、暗号化装置のセキュリティを高め、その不正防止効果を向上している。

【0038】更に、復号装置5および復号装置用ICカード15は、互いにシリアルケーブルまたはUSBケーブルなどの汎用的なインターフェースで接続され、許諾発行装置1と共有する許諾発行装置公開鍵PKL、復号装置5に固有の復号装置秘密鍵SKD、暗号化装置3と共に共有する暗号化装置鍵CKCを保持する鍵保持手段、この保持している許諾発行装置公開鍵PKLおよび利用許諾情報LMに付加された許諾電子署名SLMにより利用許諾情報LMの不正改竄を検知する利用許諾情報不正改竄検知手段、暗号化装置鍵CKCで暗号化されたコンテンツ鍵CKMを鍵保持手段に保持している暗号化装置鍵CKCで復号するコンテンツ鍵復号手段、この復号時に連続した自然数を履歴通し番号NLとして含む鍵復号履歴Hを生成する鍵復号履歴生成手段、履歴通し番号NLを保持する履歴通し番号保持手段、前記保持している復号装置秘密鍵SKDで鍵復号履歴Hに履歴電子署名SHを付加する履歴電子署名付加手段、および前記コンテンツ鍵CKMで暗号化されたデジタルコンテンツを前記復号されたコンテンツ鍵CKMで利用許諾情報LMの定義する許諾範囲に従って復号するコンテンツ復号手段を有し、これらの手段のうち、鍵保持手段、利用許諾情報不正改竄検知手段、コンテンツ鍵復号手段、鍵復号履歴生成手段、履歴通し番号保持手段、履歴電子署名付加手段をタンパフリー性ハードウェアである復号装置用ICカード15で構成し、これにより鍵保持、利用許諾情報不正改竄検知、コンテンツ鍵復号、鍵復号履歴生成、履歴通し番号保持、履歴電子署名付加をタンパフリー性ハードウェアである復号装置用ICカード15内に閉じて実行して、復号装置のセキュリティを高め、その不正防止効果を向上している。

【0039】また、検知装置7は、復号装置5と共有する復号装置公開鍵PKDおよび鍵復号履歴Hに付加された履歴電子署名SHにより鍵復号履歴Hの不正改竄を検知する鍵復号履歴不正改竄検知手段、および鍵復号履歴Hに含まれる履歴通し番号NLの連続性および復号装置5に保持している履歴通し番号NLの参照により鍵復号履歴Hの不正な抜き取りおよび不正な追加を検知する不正抜取／追加検知手段を有する。

【0040】また、デジタルコンテンツ流通業者装置9は、許諾発行装置1からの利用許諾情報LMおよび許諾電子署名SLMの収集、暗号化装置3からのコンテンツ鍵CKMで暗号化されたデジタルコンテンツM（すなわ

ち、CKM(M)）、暗号化装置鍵CKCで暗号化されたコンテンツ鍵CKM（すなわち、CKC(CKM)）の収集を行い、これらをデータベース9aに格納するとともに、復号装置5に送信して流通させるとともに、また復号装置5からの鍵復号履歴Hおよび履歴電子署名SHの収集を行い、これらをデータベース9aに格納するとともに、検知装置7に配送するように構成されている。

【0041】なお、許諾発行装置1からデジタルコンテンツ流通業者装置9への利用許諾情報LMおよび許諾電子署名SLMの受け渡しは、ネットワーク上の通信またはフロッピー（登録商標）ディスクやフラッシュメモリカードなどのような汎用的なデジタル情報記録媒体の運搬によって行われるが、本実施形態ではネットワーク上の相互認証通信を用いるものとする。

【0042】また、暗号化装置3から許諾発行装置1への利用許諾情報LMの発行要求は、本実施形態ではネットワーク上の通信を用いて行われるものとする。

【0043】暗号化装置3からデジタルコンテンツ流通業者装置9へのコンテンツ鍵CKMで暗号化されたデジタルコンテンツM（すなわち、CKM(M)）および暗号化装置鍵CKCで暗号化されたコンテンツ鍵CKM（すなわち、CKC(CKM)）の受け渡しは、ネットワーク上の通信またはフロッピーディスクやフラッシュメモリカードなどのような汎用的なデジタル情報記録媒体の運搬によって行われるが、本実施形態ではネットワーク上の相互認証通信を用いるものとする。

【0044】また、デジタルコンテンツ流通業者装置9から復号装置5への利用許諾情報LM、許諾電子署名SLM、暗号化装置鍵CKCで暗号化されたコンテンツ鍵CKM（すなわち、CKC(CKM)）、およびコンテンツ鍵CKMで暗号化されたコンテンツM（すなわち、CKM(M)）の受け渡しは、ネットワーク上の通信またはフロッピーディスクやフラッシュメモリカードなどのような汎用的なデジタル情報記録媒体の運搬によって行われるが、本実施形態ではネットワーク上の相互認証通信を用いるものとする。

【0045】更に、復号装置5からデジタルコンテンツ流通業者装置9への鍵復号履歴Hおよび履歴電子署名SHの受け渡しは、ネットワーク上の通信またはフロッピーディスクやフラッシュメモリカードなどのような汎用的なデジタル情報記録媒体の運搬によって行われるが、本実施形態ではネットワーク上の相互認証通信を用いるものとする。

【0046】デジタルコンテンツ通信業者装置9から検知装置7への鍵復号履歴Hおよび履歴電子署名SHの受け渡しは、ネットワーク上の通信またはフロッピーディスクやフラッシュメモリカードなどのような汎用的なデジタル情報記録媒体の運搬によって行われるが、本実施形態ではネットワーク上の相互認証通信を用いるものと

する。

【0047】次に、以上のように構成される本実施形態のデジタルコンテンツ流通における著作権保護システムの作用について図1内に示すステップ番号S1～S29を参照して説明する。

【0048】まず、許諾発行装置1は、暗号化装置3からの音楽デジタルコンテンツMに対する利用許諾情報LMの発行要求に応答して該利用許諾情報LMを発行する（ステップS1）。それから、許諾発行装置1に接続された許諾発行装置用ICカード11は、当該ICカード11内において許諾発行装置秘密鍵SKLを用いて、利用許諾情報LMに対する許諾電子署名SLMを生成する（ステップS3）。

【0049】次に、暗号化装置用ICカード13は、当該ICカード13内において前記デジタルコンテンツMに固有のコンテンツ鍵CKMを生成する（ステップS5）。それから、暗号化装置3は、このコンテンツ鍵CKMを用いて、デジタルコンテンツMを暗号化して、CKM(M)を生成する（ステップS7）。また、暗号化装置用ICカード13は、当該ICカード13内において暗号化装置鍵CKCを用いて、前記コンテンツ鍵CKMを暗号化して、CKC(CKM)を生成する（ステップS9）。

【0050】次に、デジタルコンテンツ流通業者装置9は、前記利用許諾情報LM、許諾電子署名SLM、暗号化装置鍵CKCで暗号化されたコンテンツ鍵CKMであるCKC(CKM)、コンテンツ鍵CKMで暗号化されたコンテンツMであるCKM(M)を収集し、これらをネットワークを介して復号装置5に配送する（ステップS11）。

【0051】復号装置5に接続された復号装置用ICカード15は、当該ICカード15内において前記利用許諾情報LM、許諾電子署名SLM、および許諾発行装置1と共に共有する許諾発行装置公開鍵PKLを用いて利用許諾情報LMの改竄を検知する（ステップS13）。この検知処理において利用許諾情報LMの改竄が検知されない場合には、暗号化装置鍵CKCで暗号化されたコンテンツ鍵CKMであるCKC(CKM)を暗号化装置鍵CKCで復号し、コンテンツ鍵CKMを生成する（ステップS15）。そして、このコンテンツ鍵CKMの復号時に連続した自然数を履歴通し番号NLとして含む鍵復号履歴Hを生成する（ステップS17）。

【0052】また、復号装置用ICカード15は、許諾発行装置に固有の復号装置秘密鍵SKDを用いて、前記鍵復号履歴Hに対する履歴電子署名SHを生成し（ステップS19）、更に鍵復号履歴Hに含まれている履歴通し番号NLを最後の履歴通し番号NLとして保持する（ステップS21）。復号装置5は、コンテンツ鍵CKMで暗号化されたデジタルコンテンツMであるCKM(M)をステップS15で復号されたコンテンツ鍵CK

Mを用いて利用許諾情報LMの定義する許諾範囲に従つて復号して、デジタルコンテンツMを生成する（ステップS23）。

【0053】次に、デジタルコンテンツ流通業者装置9は、復号装置5から鍵復号履歴Hおよび履歴電子署名SHを収集して、データベース9aに格納する（ステップS25）。

【0054】それから、検知装置7は、デジタルコンテンツ流通業者装置9から受け取った鍵復号履歴Hおよび履歴電子署名SH、および復号装置5と共有している復号装置公開鍵PKDを用いて、鍵復号履歴Hの改竄を検知する（ステップS27）。また、検知装置7は、鍵復号履歴Hおよびその前後の鍵復号履歴が含む履歴通し番号の連続性および復号装置5に保持している履歴通し番号NLを参照して、鍵復号履歴Hの不正な抜き取りおよび不正な追加を検知する（ステップS29）。

【0055】上述したように、音楽デジタルコンテンツMを利用許諾情報LMの定める許諾範囲内でのみ利用可能とし、この許諾範囲を逸脱したデジタルコンテンツMの不正利用を検知し、デジタルコンテンツ流通業者の水増し請求やデジタルコンテンツ利用者の利用否認による支払い拒否などを防止することができる音楽デジタルコンテンツ流通サービスを実現することができる。

【0056】また、上記実施形態では、復号装置5は、復号時に許諾発行装置1などの外部と接続されている必要がないし、また検知装置7による鍵復号履歴Hの収集は復号時である必要はないため、復号装置5は復号時に検知装置7に接続されている必要もない。

【0057】次に、図2を参照して、本発明の他の実施形態に係るデジタルコンテンツ流通における著作権保護システムについて説明する。

【0058】図2に示す実施形態の著作権保護システムは、図1に示した実施形態における許諾発行装置1、暗号化装置3、および復号装置5をそれぞれ演算機能および記憶機能において分割して構成されるタンパクリー性ハードウェアを構成する許諾発行装置用ICカード1、暗号化装置用ICカード13、および復号装置用ICカード15を使用する代わりに、許諾発行装置、暗号化装置、および復号装置で共有する秘密情報鍵CKSを使用し、この秘密情報鍵CKSで許諾発行装置秘密鍵SKL、暗号化装置鍵CKC、復号装置秘密鍵SKD、および履歴通し番号NLを暗号化するように構成した点が異なるものであり、この構成および作用は図1の実施形態と同じである。

【0059】すなわち、図2に示す著作権保護システムは、ICカードでそれぞれ分割されていない許諾発行装置10、暗号化装置30および復号装置50、検知装置7、およびデジタルコンテンツ流通業者装置9から構成されている。そして、許諾発行装置10は、許諾発行装置秘密鍵SKLを秘密情報鍵CKSで暗号化したCKS

(SLK)を保持する手段を有し、暗号化装置30は、暗号化装置鍵CKCを秘密情報鍵CKSで暗号化したCKS(CKC)を保持する手段を有し、復号装置50は、暗号化装置鍵CKC、復号装置秘密鍵SKD、履歴通し番号NLを秘密情報鍵CKSで暗号化したCKS(CKC)、CKS(SKD)、CKS(NL)を保持する手段を有する。

【0060】なお、許諾発行装置10からデジタルコンテンツ流通業者装置9への利用許諾情報LMおよび許諾電子署名SLMの受け渡しは、ネットワーク上の通信またはフロッピーディスクやフラッシュメモリカードなどのような汎用的なデジタル情報記録媒体の運搬によって行われるが、本実施形態ではネットワーク上の相互認証通信を用いるものとする。

【0061】また、暗号化装置30から許諾発行装置10への利用許諾情報LMの発行要求は、本実施形態ではネットワーク上の通信を用いて行われるものとする。

【0062】暗号化装置30からデジタルコンテンツ流通業者装置9へのコンテンツ鍵CKMで暗号化されたデジタルコンテンツMであるCKM(M)および暗号化装置鍵CKCで暗号化されたコンテンツ鍵CKMであるCKC(CKM)の受け渡しは、ネットワーク上の通信またはフロッピーディスクやフラッシュメモリカードなどのような汎用的なデジタル情報記録媒体の運搬によって行われるが、本実施形態ではネットワーク上の相互認証通信を用いるものとする。

【0063】また、デジタルコンテンツ流通業者装置9から復号装置50への利用許諾情報LM、許諾電子署名SLM、暗号化装置鍵CKCで暗号化されたコンテンツ鍵CKMであるCKC(CKM)、およびコンテンツ鍵CKMで暗号化されたコンテンツMであるCKM(M)の受け渡しは、ネットワーク上の通信またはフロッピーディスクやフラッシュメモリカードのような汎用的なデジタル情報記録媒体の運搬によって行われるが、本実施形態ではネットワーク上の相互認証通信を用いるものとする。

【0064】更に、復号装置50からデジタルコンテンツ流通業者装置9への鍵復号履歴Hおよび履歴電子署名SHの受け渡しは、ネットワーク上の通信またはフロッピーディスクやフラッシュメモリカードなどのような汎用的なデジタル情報記録媒体の運搬によって行われるが、本実施形態ではネットワーク上の相互認証通信を用いるものとする。

【0065】デジタルコンテンツ流通業者装置9から検知装置7への鍵復号履歴Hおよび履歴電子署名SHの受け渡しは、ネットワーク上の通信またはフロッピーディスクやフラッシュメモリカードなどのような汎用的なデジタル情報記録媒体の運搬によって行われるが、本実施形態ではネットワーク上の相互認証通信を用いるものとする。

【0066】次に、以上のように構成される本実施形態のデジタルコンテンツ流通における著作権保護システムの作用について図2内に示すステップ番号S31～S59を参照して説明する。

【0067】まず、許諾発行装置10は、暗号化装置30からの音楽デジタルコンテンツMに対する利用許諾情報LMの発行要求に応答して該利用許諾情報LMを発行する(ステップS31)。それから、許諾発行装置10は、当該許諾発行装置10内に隠蔽された秘密情報鍵CKSおよび許諾発行装置秘密鍵SKLを用いて、利用許諾情報LMに対する許諾電子署名SLMを生成する(ステップS33)。

【0068】次に、暗号化装置30は、前記デジタルコンテンツMに固有のコンテンツ鍵CKMを生成する(ステップS35)。それから、暗号化装置30は、このコンテンツ鍵CKMを用いて、デジタルコンテンツMを暗号化して、CKM(M)を生成する(ステップS37)。また、暗号化装置30は、当該暗号化装置30内に隠蔽された秘密情報鍵CKSで暗号化された暗号化装置鍵CKCであるCKS(CKC)を用いて、前記コンテンツ鍵CKMを暗号化して、CKC(CKM)を生成する(ステップS39)。

【0069】次に、デジタルコンテンツ流通業者装置9は、前記利用許諾情報LM、許諾電子署名SLM、暗号化装置鍵CKCで暗号化されたコンテンツ鍵CKMであるCKC(CKM)、コンテンツ鍵CKMで暗号化されたコンテンツMであるCKM(M)を収集し、これらをネットワークを介して復号装置50に配達する(ステップS41)。

【0070】復号装置50は、前記利用許諾情報LM、許諾電子署名SLM、および許諾発行装置10と共有する許諾発行装置公開鍵PKLを用いて利用許諾情報LMの改竄を検知する(ステップS43)。この検知処理において利用許諾情報LMの改竄が検知されない場合には、暗号化装置鍵CKCで暗号化されたコンテンツ鍵CKMであるCKC(CKM)を当該復号装置50内に隠蔽された秘密情報鍵CKSで暗号化された暗号化装置鍵CKCであるCKS(CKC)で復号して、コンテンツ鍵CKMを生成する(ステップS45)。そして、このコンテンツ鍵CKMの復号時に連続した自然数を履歴通し番号NLとして含む鍵復号履歴Hを生成する(ステップS47)。

【0071】また、復号装置50は、当該復号装置50内に隠蔽された秘密情報鍵CKSで暗号化された復号装置秘密鍵SKDであるCKS(SKD)を用いて、前記鍵復号履歴Hに対する履歴電子署名SHを生成し(ステップS49)、更に鍵復号履歴Hに含まれている履歴通し番号NLを当該復号装置50内に隠蔽する秘密情報鍵CKSで暗号化してCKS(NL)を生成し、暗号化された最後の履歴通し番号CKS(NL)として保持する

(ステップS51)。復号装置50は、コンテンツ鍵CKMで暗号化されたデジタルコンテンツMであるCKM(M)をステップS45で復号されたコンテンツ鍵CKMを用いて利用許諾情報LMの定義する許諾範囲に従って復号して、デジタルコンテンツMを生成する(ステップS53)。

【0072】次に、デジタルコンテンツ流通業者装置9は、復号装置50から鍵復号履歴Hおよび履歴電子署名SHを収集して、データベース9aに格納する(ステップS55)。

【0073】それから、検知装置7は、デジタルコンテンツ流通業者装置9から受け取った鍵復号履歴Hおよび履歴電子署名SH、および復号装置50と共にしている復号装置公開鍵PKDを用いて、鍵復号履歴Hの改竄を検知する(ステップS57)。また、検知装置7は、鍵復号履歴Hおよびその前後の鍵復号履歴が含む履歴通し番号の連続性および復号装置50に保持している履歴通し番号NLを参照して、鍵復号履歴Hの不正な抜き取りおよび不正な追加を検知する(ステップS59)。

【0074】上述したように、音楽デジタルコンテンツMを利用許諾情報LMの定める許諾範囲内でのみ利用可能とし、この許諾範囲を逸脱したデジタルコンテンツMの不正利用を検知し、デジタルコンテンツ流通業者の水増し請求やデジタルコンテンツ利用者の利用否認による支払い拒否などを防止することができる音楽デジタルコンテンツ流通サービスを実現することができる。

【0075】なお、上記実施形態において、許諾発行装置10、暗号化装置30、復号装置50のいずれかで秘密情報鍵CKSを用いる代わりに、図1の実施形態で説明したタンパフリー性ハードウェアであるICカードを接続して構成される著作権保護システムを実現することも可能であることは明らかなことである。すなわち、許諾発行装置10、暗号化装置30、復号装置50のうちいずれかの1つまたは2つが秘密情報鍵CKSを用いる代わりに、図1に示したように演算機能や記憶機能で分割し、この機能を有するタンパフリー性ハードウェアであるICカードを接続して構成してもよいものである。

【0076】なお、上述した各実施形態では、コンテンツが音楽デジタルコンテンツMである場合について説明したが、本発明はこのような音楽デジタルコンテンツに限定されるものではなく、その他のコンテンツにも適用可能なものである。

【0077】

【発明の効果】以上説明したように、本発明によれば、許諾発行装置はデジタルコンテンツに対して許諾範囲を定義した利用許諾情報を発行し、利用許諾情報に対する許諾電子署名を生成し、復号装置は許諾発行装置公開鍵および許諾電子署名により利用許諾情報の不正改竄を検知するとともに、暗号化されたコンテンツを利用許諾情報の定義する許諾範囲に従って復号するので、デジタル

コンテンツを許諾範囲内のみで利用可能とし、許諾範囲を逸脱した不正利用を検知して防止することができ、またネットワーク上の相互認証通信によるトラヒックの増加およびサービスコストの増加、ネットワーク非接続時のコンテンツ利用不可という従来の問題を解決できる。また、復号装置は復号時に許諾発行装置などの外部と接続されている必要がない。

【0078】また、本発明によれば、検知装置は復号装置公開鍵および鍵復号履歴に付加された履歴電子署名により鍵復号履歴の不正改竄を検知し、鍵復号履歴に含まれる履歴通し番号の連続性および復号装置に保持している履歴通し番号の参照により鍵復号履歴の不正な抜き取りおよび不正な追加を検知するので、デジタルコンテンツ流通業者の水増し請求やデジタルコンテンツ利用者の利用否認による支払い拒否などを防止することができ、またコンテンツ利用後の利用履歴抜き取りまたは改竄によるデジタルコンテンツの不正利用を検知して防止できる。更に、検知装置による鍵復号履歴の収集は復号時である必要はなく、復号装置は復号時に検知装置に接続されている必要がない。

【0079】更に、本発明によれば、許諾発行装置はデジタルコンテンツに対して許諾範囲を定義した利用許諾情報を発行し、利用許諾情報に対する許諾電子署名を生成し、暗号化装置はコンテンツ鍵を生成してコンテンツを暗号化し、コンテンツ鍵を暗号化し、復号装置は許諾発行装置公開鍵および利用許諾情報に付加された許諾電子署名により利用許諾情報の不正改竄を検知し、暗号化されたコンテンツ鍵を復号し、この復号時に連続した履歴通し番号を含む鍵復号履歴を生成し、鍵復号履歴に履歴電子署名を付加し、暗号化されたデジタルコンテンツを利用許諾情報の定義する許諾範囲に従って復号し、検知装置は復号装置公開鍵および鍵復号履歴に付加された履歴電子署名により鍵復号履歴の不正改竄を検知し、鍵復号履歴に含まれる履歴通し番号の連続性および復号装置に保持している履歴通し番号の参照により鍵復号履歴の不正な抜き取りおよび不正な追加を検知するので、デジタルコンテンツを許諾範囲内のみで利用可能とし、許諾範囲を逸脱した不正利用を検知して防止することができ、デジタルコンテンツ流通業者の水増し請求やデジタルコンテンツ利用者の利用否認による支払い拒否などを防止することができるとともに、コンテンツ利用後の利用履歴抜き取りまたは改竄によるデジタルコンテンツの不正利用を検知して防止でき、またネットワーク上の相互認証通信によるトラヒックの増加およびサービスコストの増加、ネットワーク非接続時のコンテンツ利用不可という従来の問題を解決できる。

【0080】本発明によれば、暗号化装置はコンテンツ鍵生成、コンテンツ鍵暗号化、および暗号化装置鍵保持をタンパフリーアル性ハードウェア内に閉じて実行するので、暗号化装置のセキュリティを高め、その不正防止効

果を向上することができる。

【0081】また、本発明によれば、許諾発行装置は許諾発行装置秘密鍵保持および許諾電子署名生成付与をタンパフリーアル性ハードウェア内に閉じて実行するので、許諾発行装置のセキュリティを高め、その不正防止効果を向上することができる。

【0082】更に、本発明によれば、復号装置は鍵保持、利用許諾情報不正改竄検知、コンテンツ鍵復号、鍵復号履歴生成、履歴通し番号保持、履歴電子署名付加をタンパフリーアル性ハードウェア内に閉じて実行するので、復号装置のセキュリティを高め、その不正防止効果を向上することができる。

【0083】本発明によれば、暗号化装置、許諾発行装置、および復号装置は秘密情報鍵を共有し、暗号化装置は暗号化装置鍵を秘密情報鍵で暗号化して保持し、許諾発行装置は許諾発行装置秘密鍵を秘密情報鍵で暗号化して保持し、復号装置は暗号化装置鍵、復号装置秘密鍵、履歴通し番号を秘密情報鍵で暗号化して保持するので、暗号化装置、許諾発行装置、および復号装置のそれぞれのセキュリティを高め、その不正防止効果を向上することができる。

【0084】また、本発明によれば、暗号化装置はコンテンツ鍵生成、コンテンツ鍵暗号化、および暗号化装置鍵保持をタンパフリーアル性ハードウェア内に閉じて実行し、許諾発行装置および復号装置は秘密情報鍵を共有し、許諾発行装置は許諾発行装置秘密鍵を秘密情報鍵で暗号化して保持し、復号装置は暗号化装置鍵、復号装置秘密鍵、履歴通し番号を秘密情報鍵で暗号化して保持するので、暗号化装置、許諾発行装置、および復号装置のそれぞれのセキュリティを高め、その不正防止効果を向上することができる。

【0085】更に、本発明によれば、許諾発行装置は許諾発行装置秘密鍵保持手段および許諾電子署名生成付与をタンパフリーアル性ハードウェア内に閉じて実行し、暗号化装置および復号装置は秘密情報鍵を共有し、暗号化装置は暗号化装置鍵を秘密情報鍵で暗号化して保持し、復号装置は暗号化装置鍵、復号装置秘密鍵、履歴通し番号を秘密情報鍵で暗号化して保持するので、暗号化装置、許諾発行装置、および復号装置のそれぞれのセキュリティを高め、その不正防止効果を向上することができる。

【0086】本発明によれば、復号装置は鍵保持、利用許諾情報不正改竄検知、コンテンツ鍵復号、鍵復号履歴生成、履歴通し番号保持、履歴電子署名付加をタンパフリーアル性ハードウェア内に閉じて実行し、暗号化装置および許諾発行装置は秘密情報鍵を共有し、暗号化装置は暗号化装置鍵を秘密情報鍵で暗号化して保持し、許諾発行装置は許諾発行装置秘密鍵を秘密情報鍵で暗号化して保持するので、暗号化装置、許諾発行装置、および復号装置のそれぞれのセキュリティを高め、その不正防止効果を向上することができる。

【0087】また、本発明によれば、暗号化装置は暗号化装置鍵を秘密情報鍵で暗号化して保持し、許諾発行装置は許諾発行装置秘密鍵保持および許諾電子署名生成付与をタンパフリーア性ハードウェア内に閉じて実行し、復号装置は鍵保持、利用許諾情報不正改竄検知、コンテンツ鍵復号、鍵復号履歴生成、履歴通し番号保持、履歴電子署名付加をタンパフリーア性ハードウェア内に閉じて実行するので、暗号化装置、許諾発行装置、および復号装置のそれぞれのセキュリティを高め、その不正防止効果を向上することができる。

【0088】更に、本発明によれば、許諾発行装置は許諾発行装置秘密鍵を秘密情報鍵で暗号化して保持し、暗号化装置はコンテンツ鍵生成、コンテンツ鍵暗号化、および暗号化装置鍵保持をタンパフリーア性ハードウェア内に閉じて実行し、復号装置は鍵保持、利用許諾情報不正改竄検知、コンテンツ鍵復号、鍵復号履歴生成、履歴通し番号保持、履歴電子署名付加をタンパフリーア性ハードウェア内に閉じて実行するので、暗号化装置、許諾発行装置、および復号装置のそれぞれのセキュリティを高め、その不正防止効果を向上することができる。

【0089】本発明によれば、復号装置は暗号化装置鍵、復号装置秘密鍵、履歴通し番号を秘密情報鍵で暗号化して保持し、暗号化装置はコンテンツ鍵生成、コンテ

ンツ鍵暗号化、および暗号化装置鍵保持をタンパフリーア性ハードウェア内に閉じて実行し、許諾発行装置は許諾発行装置秘密鍵保持および許諾電子署名生成付与をタンパフリーア性ハードウェア内に閉じて実行するので、暗号化装置、許諾発行装置、および復号装置のそれぞれのセキュリティを高め、その不正防止効果を向上することができる。

【図面の簡単な説明】

【図1】本発明の一実施形態に係るデジタルコンテンツ流通における著作権保護システムの構成を示す図である。

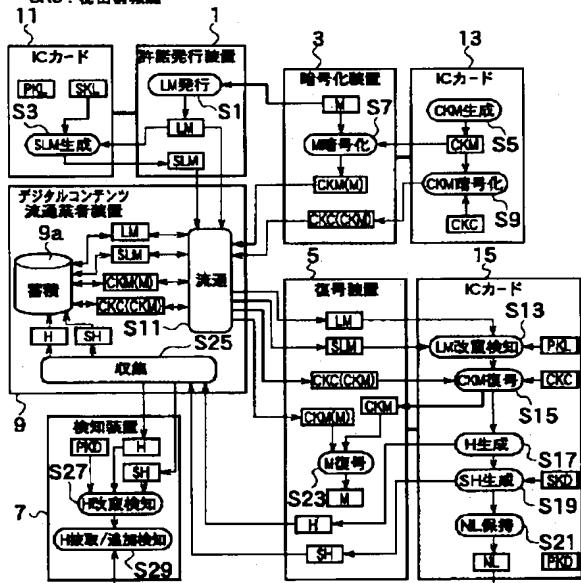
【図2】本発明の他の実施形態に係るデジタルコンテンツ流通における著作権保護システムの構成を示す図である。

【符号の説明】

- 1, 10 許諾発行装置
- 3, 30 暗号化装置
- 5, 50 復号装置
- 7 検知装置
- 9 デジタルコンテンツ流通業者装置
- 11 許諾発行装置用ICカード
- 13 暗号化装置用ICカード
- 15 復号装置用ICカード

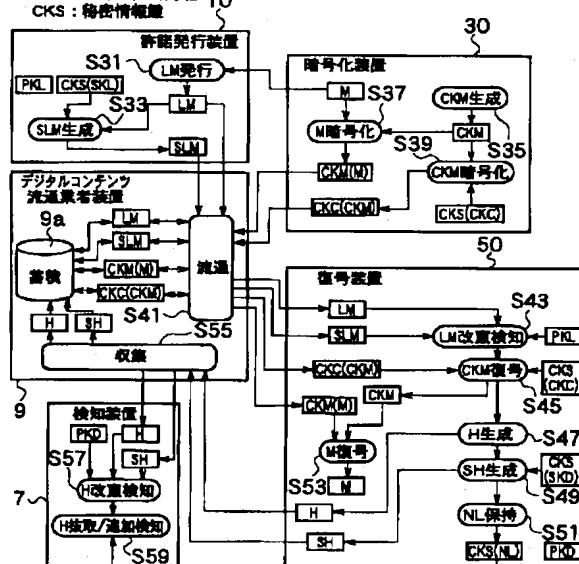
【図1】

M : 音楽デジタルコンテンツ
 LM : Mに対して発行された
 利用許諾情報
 SLM : LMに対する許諾電子署名
 CKM : Mに対するコンテンツ鍵
 H : 設定履歴
 NL : 僅号装置に保持される最後の履歴送し番号
 SH : Hに対する履歴電子署名
 SKL : 許諾発行装置秘密鍵
 PKL : 許諾発行装置公開鍵
 CKC : 密号化装置
 SKD : 僅号装置秘密鍵
 PKD : 僅号装置公開鍵
 CKS : 秘密情報鍵



【図2】

M : 音楽デジタルコンテンツ
 LM : Mに対して発行された
 利用許諾情報
 SLM : LMに対する許諾電子署名
 CKM : Mに対するコンテンツ鍵
 H : 設定履歴
 NL : 僅号装置に保持される最後の履歴送し番号
 SH : Hに対する履歴電子署名
 SKL : 許諾発行装置秘密鍵
 PKL : 許諾発行装置公開鍵
 CKC : 密号化装置
 SKD : 僅号装置秘密鍵
 PKD : 僅号装置公開鍵
 CKS : 秘密情報鍵



フロントページの続き

(51) Int. Cl. 7

G 06 K 19/10

H 04 L 9/08

識別記号

F I

マーク (参考)

G 06 K 19/00

R

H 04 L 9/00

601B

F ターム (参考) 5B017 AA03 AA06 AA08 BA07 BA09
 CA14
 5B035 AA13 BB09 BC00 CA11
 5B058 CA27 KA02 KA04 KA08 KA31
 KA35 YA20
 5J104 AA09 LA03 LA06 NA02 NA35
 NA42